EXHIBIT D

Are voting-machine modems truly divorced from the Internet?

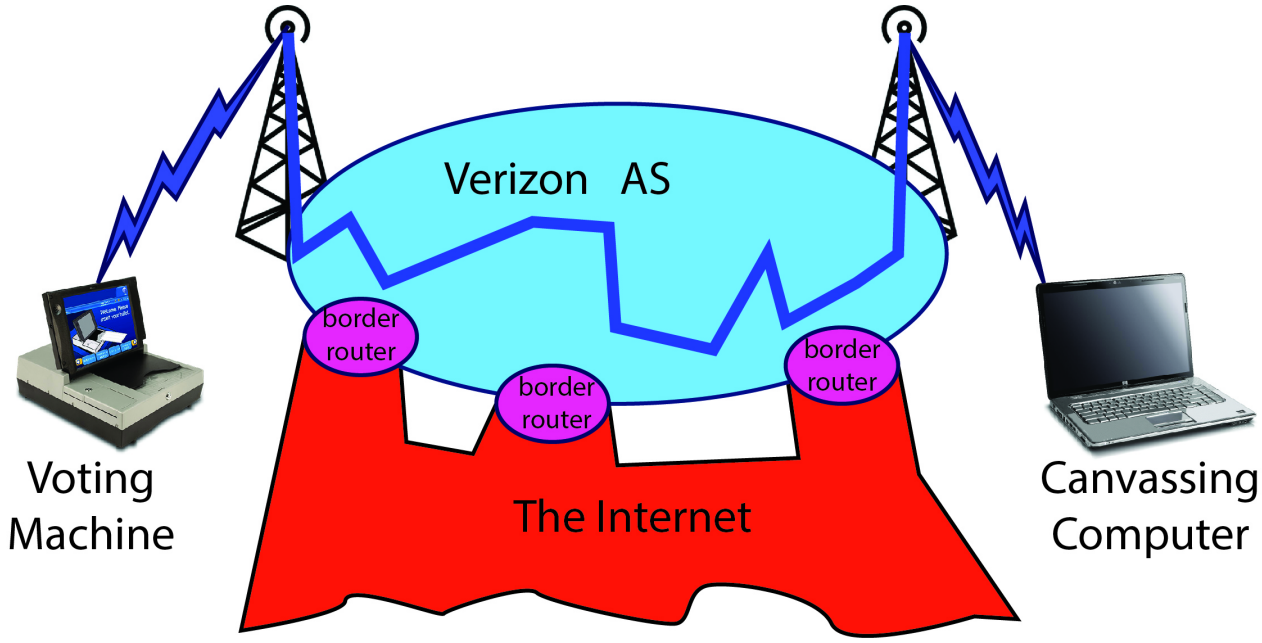
FEBRUARY 22, 2018 BY ANDREW APPEL

*(This article is written jointly with my colleague **Kyle Jamieson**, who specializes in wireless networks.)*

[See also: **The myth of the hacker-proof voting machine**]

The ES&S model DS200 optical-scan voting machine has a cell-phone modem that it uses to upload election-night results from the voting machine to the "county central" canvassing computer. We know it's a bad idea to connect voting machines (and canvassing computers) to the Internet, because this allows their vulnerabilities to be exploited by hackers anywhere in the world. (In fact, a judge in New Jersey ruled in 2009 that the state must not connect its voting machines and canvassing computers to the internet, for that very reason.) So the question is, does DS200's cell-phone modem, in effect, connect the voting machine to the Internet?

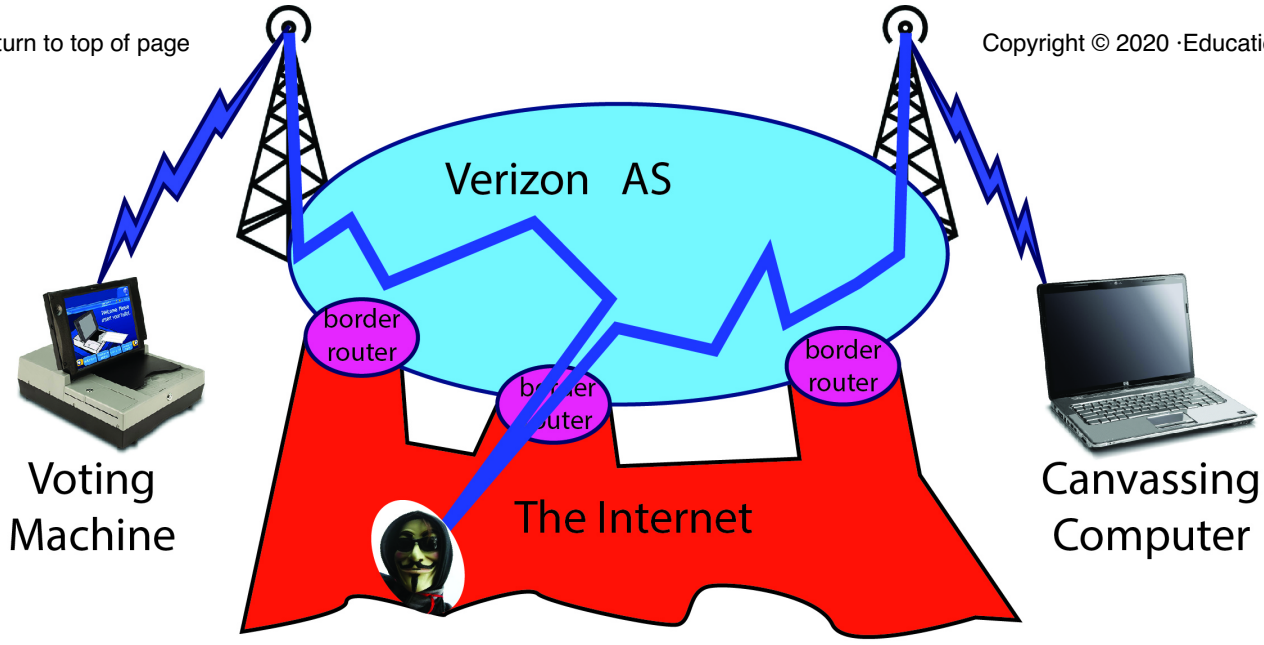
The vendor (ES&S) and the counties that bought the machine say, "no, it's an *analog* modem." That's not true; it appears to be a **Multitech MTSMC-C2-N3**-R.1 (Verizon C2 series modem), a fairly complex digital device. But maybe what they mean is "it's just a phone call, not really the Internet." So let's review how phone calls work:



The voting machine calls the county-central computer using its cell-phone modem to the nearest tower; this connects through Verizon's "Autonomous System" (AS), part of the packet-switched Internet, to a cell tower (or land-line station) near the canvassing computer.

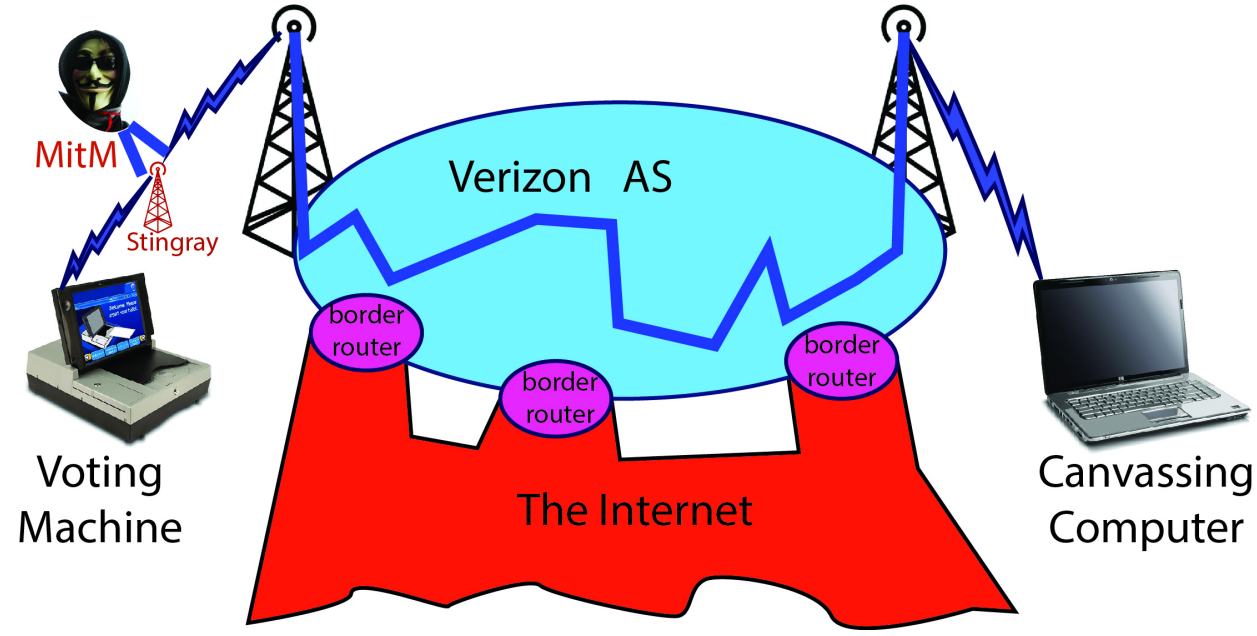
Verizon attempts to control access to the routers internal to its own AS, using firewall rules on the border routers. Each border router runs (probably) millions of lines of software; as such it is subject to bugs and vulnerabilities. If a hacker finds one of these vulnerabilities, he can modify messages as they transit the AS network:

Return to top of page

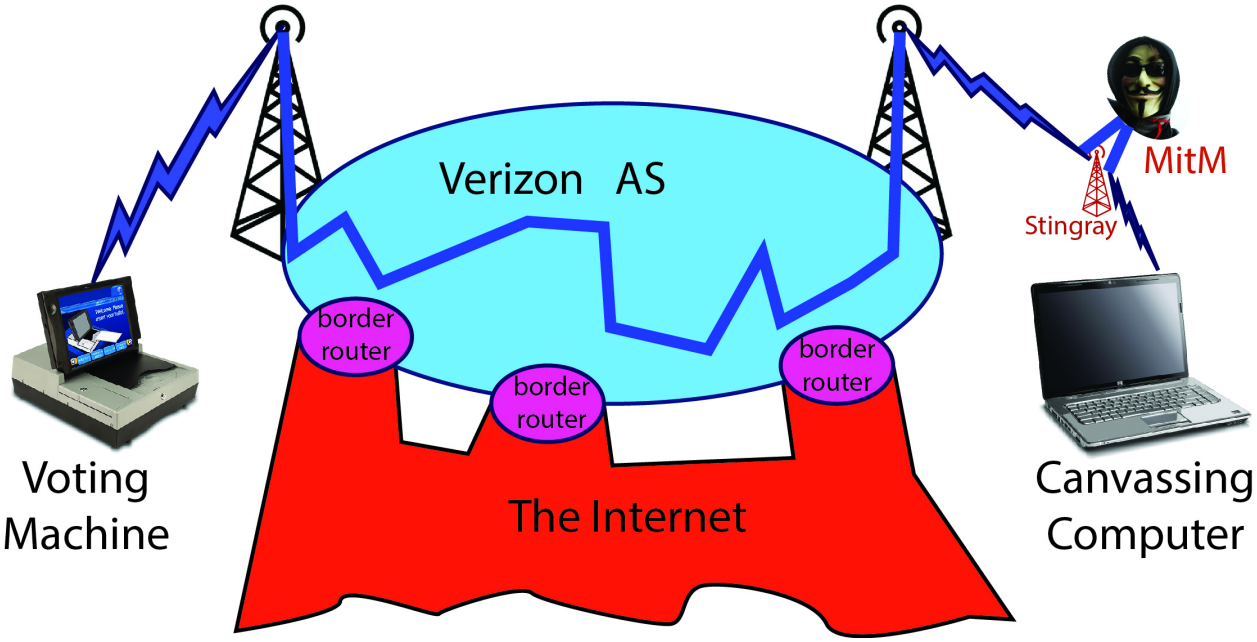


Do border routers actually have vulnerabilities in practice? Of course they do! US-CERT has **highlighted this as an issue of importance**. It would surprising if the Russian mafia or the FBI were not equipped to exploit such vulnerabilities.

Even easier than hacking through router bugs is just setting up an imposter cell-phone "tower" near the voting machine; one commonly used brand of these, used by many police departments, is called "Stingray."



I've labelled the hacker as "MitM" for "man-in-the-middle." He is well positioned to alter vote totals as they are uploaded. Of course, he will do better to put his Stingray near the county-central canvassing computer, so he can hack all the voting machines in the county, not just one near his Stingray:



So, in summary: phone calls are *not* unconnected to the Internet; the hacking of phone calls is easy (police departments with Stingray devices do it all the time); and even between the cell-towers (or land-line stations), your calls go over parts of the Internet. If your state laws, or a court with jurisdiction, say not to connect your voting machines to the Internet, then you probably shouldn't use telephone modems either.

FILED UNDER: OTHER TOPICS TAGGED WITH: VOTING MACHINES, VOTING SECURITY